OMI FOUNDATION

India’s Digital Future: Strengthening DPDP Rules for Privacy, Innovation, and Global Leadership

Position Paper

April 2025
CTT PP 25/03
Centre for Technology Transitions

India’s Digital Future:

Strengthening DPDP Rules for Privacy, Innovation, and Global Leadership

Position Paper

April 2025

OMI FOUNDATION

Table of Contents

Executive Summary

India's Opportunity: Strengthening DPDP Rules for Global Leadership in Digital Privacy & Inclusive Growth

The Draft Digital Personal Data Protection (DPDP) Rules, 2025, issued under the Digital Personal Data Protection Act, 2023, present a historic opportunity for India to shape the future of digital privacy governance while unlocking new pathways for innovation-driven economic growth. As one of the world's fastest-growing digital economies - home to a thriving startup ecosystem, a booming AI sector, and cutting-edge digital public infrastructure - India can set a global benchmark by crafting a data protection framework that safeguards individual rights without stifling innovation.

However, for India to emerge as a global leader in data governance, the draft rules must address critical gaps that could erode citizen trust, increase compliance burdens for businesses, and limit India's global competitiveness.

Key Gaps in the Draft Rules

1. **Limited Protections for Sensitive Data:** The draft rules fail to differentiate between sensitive personal data (e.g., health, biometric, and financial data) and general personal data, lacking enhanced safeguards for high-risk categories.
2. **Unclear Framework for Cross-Border Data Transfers:** The draft rules leave India's approach to international data flows undefined, creating uncertainty for IT, fintech, and AI firms operating in global markets.
3. **Lack of Sector-Specific Standards:** Unlike global best practices (e.g., GDPR, Singapore's PDPA), India's rules apply a one-size-fits-all approach to data regulation, overlooking the need for stricter safeguards in finance, healthcare, EdTech, and digital payments.
4. **Weak Algorithmic Accountability & AI Governance:** The draft rules do not mandate transparency in AI-driven decision-making, leaving risks of bias in credit scoring, insurance pricing, and automated hiring unaddressed.
5. **High Compliance Burden for MSMEs & Startups:** Small businesses and early-stage enterprises face disproportionate regulatory obligations, with insufficient clarity on scaled compliance frameworks.
6. **Gaps in Grievance Redressal & Regulatory Oversight:** The Data Protection Board of India (DPBI) lacks public accountability and is not required to publish decisions, penalties, or regulatory guidance, undermining transparency and trust.

Methodology: A Dual-Lens Approach to Evaluating the DPDP Rules

This analysis employs a dual-framework methodology to assess the Draft Digital Personal Data Protection (DPDP) Rules, 2025 from both a rights-based and socio-technical systems (STS) perspective:

- **Rights-Based Approach:** Evaluates the DPDP Rules against fundamental rights, data-specific rights, and emerging digital rights to ensure alignment with constitutional principles, international privacy laws (GDPR, CCPA, PDPA), and sectoral best practices.
- **Socio-Technical Systems (STS) Framework:** Examines the real-world feasibility of implementing the rules, analyzing regulatory capacity, compliance costs, technological constraints, and institutional readiness. This ensures that policy recommendations are not just legally sound but also practically viable for India’s diverse digital ecosystem.

By combining these complementary perspectives, this report provides a comprehensive evaluation of the DPDP Rules, identifying key gaps and proposing strategic reforms that will help India build a globally competitive and privacy-centric digital economy.

Strategic Recommendations to Maximize India’s Digital Advantage

To position India as a trusted global hub for privacy-centric digital innovation, the DPDP Rules must integrate the following critical reforms.

1. **Strengthen Protections for Sensitive Data:** Establish stricter security and consent requirements for financial, health, and biometric data to align with global privacy standards.
2. **Enable Cross-Border Data Transfers While Safeguarding National Interests:** Develop a risk-based data transfer framework to facilitate global business operations while ensuring regulatory oversight.
3. **Introduce Sector-Specific Data Protection Standards:** Implement tailored compliance frameworks for finance, digital health, EdTech, and public services to enhance security and build global trust in India’s enterprises.
4. **Mandate Algorithmic Transparency & Fairness in AI Systems:** Require AI bias audits and explainability standards to prevent discriminatory outcomes in hiring, lending, and government decision-making.
5. **Ease Compliance Burdens for MSMEs & Startups:** Introduce a tiered compliance model where smaller businesses have simplified regulatory obligations, allowing them to focus on growth and innovation.
6. **Enhance DPBI’s Role & Accountability:** Require the Data Protection Board to publish enforcement actions, conduct independent audits, and maintain transparency in its decision-making.

7. **Strengthen Grievance Redressal & Accessibility:** Mandate strict response timelines (15 days for data fiduciaries, 30 days for DPBI) and introduce offline dispute resolution mechanisms for digitally excluded communities.

India's Path to Global Leadership in Data Governance

India stands at a defining moment in shaping the world's next-generation data protection framework. Here's an opportunity for India to establish a globally competitive, innovation-friendly, and rights-driven data protection regime. By strengthening rights protections, fostering innovation-friendly regulations, and introducing sectoral best practices, India can create a globally competitive and privacy-respecting digital economy. The DPDP Rules must do more than ensure privacy - they must position India as the preferred destination for ethical AI, digital payments, and cross-border data governance.

By embedding these strategic reforms, India can:

- Enhance global trust in its digital economy, attracting investment and innovation.
- Lead the world in AI ethics, data fairness, and digital rights governance.
- Safeguard individual privacy while fostering responsible data-driven growth.

India has the capability, the ambition, and the moment to set a new global benchmark - one that balances economic opportunity, technological leadership, and privacy protection. The time to act is now.

1. Introduction

The rapid growth of digital technology has fundamentally transformed how personal data is collected, processed, and used. In India, this shift has been driven by increased digital adoption across sectors, accelerated by initiatives like Digital India, the rise of the platform economy, and the proliferation of social media platforms. While these advancements have unlocked immense economic and social potential, they have also raised critical concerns about data privacy, misuse, and the need for robust legal frameworks to safeguard individual rights.

Recognising the importance of personal data protection, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), a landmark piece of legislation aimed at creating a comprehensive legal framework to regulate personal data processing (Government of India, 2023). To operationalise this act, the Government of India has introduced the Draft Digital Personal Data Protection Rules, 2025, which lay out detailed guidelines on various aspects, including consent mechanisms, obligations of data fiduciaries, rights of individuals (data principals), and regulatory oversight mechanisms (Government of India, 2025).

India's efforts to establish a robust data protection regime align with global trends, such as the European Union's General Data Protection Regulation (GDPR) and the United States' California Consumer Privacy Act (CCPA). However, the DPDP Act and its accompanying rules aim to address India's unique digital ecosystem, characterised by a diverse population, varying levels of digital literacy, and a growing emphasis on data-driven innovation.

At this critical juncture, the draft rules offer an opportunity to bridge gaps in India's data governance landscape while ensuring a balance between individual privacy rights and economic growth. However, their successful implementation will depend on addressing key challenges, such as compliance burdens on businesses, enforcement capacity of the Data Protection Board, and clarity in the operational provisions, among others.

This position paper aims to provide an in-depth review of the draft rules, assess their alignment with international best practices, and propose actionable recommendations to strengthen their effectiveness. By doing so, the paper seeks to contribute to India's journey toward becoming a global leader in data governance and privacy innovation.

2. Methodology: A Dual Approach to Evaluating the DPDP Rules

2.1. Analytical Frameworks for Assessing the Draft DPDP Rules

To provide a holistic and actionable analysis of the Draft Digital Personal Data Protection (DPDP) Rules, 2025, this paper employs a dual-framework approach:

1. **The Rights-Based Approach:** Evaluates the draft rules through the lens of fundamental rights, data-specific rights, and contextual rights, ensuring that they uphold privacy, fairness, and transparency for individuals.
2. **The Socio-Technical Systems (STS) Framework:** Examines the practical implementation and systemic challenges of the draft rules by analyzing the interactions between legal, institutional, and technological infrastructures.

By integrating these perspectives, this analysis assesses not only the legal sufficiency of the rules but also their real-world impact on individuals, businesses, and governance structures.

2.2. Rights-Based Approach: Evaluating the Rules Against Core Data Protection Principles

This framework assesses whether the DPDP Rules protect individual rights effectively. It applies a three-tiered rights structure:

1. First-Order Rights (Direct Individual Entitlements): Rights that directly empower individuals to control, access, or restrict their data.
    a. Fundamental Rights (Privacy, Equality, Freedom of Expression, Life & Dignity)
    b. Data-Specific Rights (Access, Correction, Erasure, Transparency, Portability, Restriction of Processing)
    c. Context-Specific Rights (Children's Rights, Rights of Vulnerable Groups, Rights in Public-Private Interactions)
2. Second-Order Rights (Mechanisms for Rights Enforcement): Ensures that first-order rights are practically enforceable by:
    a. Strengthening Governance & Accountability (Fair Processing, Due Process, Remedies, Compensation)
    b. Ensuring Regulatory Oversight (Transparency, Public Accountability of the DPBI, Participatory Policymaking)
    c. Mandating Audit & Risk Assessments (Impact Assessments, Compliance Monitoring)
3. Emerging & Sector-Specific Rights: Adapting the rules to new technologies and industries, such as:

   a. AI & Algorithmic Fairness (Right Against Automated Profiling, Right to Explainability)
   b. Blockchain & Data Immutability (Addressing Erasure Challenges)
   c. Biometric Data Protections (Safeguards Against Facial Recognition Misuse)
   d. Sector-Specific Rights (Finance, Health, EdTech, Public Services)

This rights-based lens ensures that data protection is aligned with constitutional values, individual autonomy, and international best practices.

2.3. Socio-Technical Systems (STS) Framework: Evaluating Systemic Feasibility & Challenges

While a rights-based analysis ensures legal sufficiency, the STS framework examines whether the rules can be effectively implemented within India’s unique digital ecosystem.

1. Mapping Key Stakeholders & Institutions: The STS framework evaluates how different actors interact within the data governance ecosystem:
   a. Regulatory Bodies (MeitY, DPBI, Sectoral Regulators)
   b. Data Fiduciaries (Tech Platforms, Banks, Health Providers, Government Agencies)
   c. Consent Managers & Data Processors (Intermediaries Managing Compliance)
   d. Data Principals (Individuals & Communities)
2. Assessing Implementation Barriers
   a. Are the compliance requirements practical for businesses (especially MSMEs & startups)?
   b. Are there adequate institutional safeguards for enforcement & dispute resolution?
   c. How do the rules impact technological systems (AI, fintech, health data, digital platforms)?
   d. Are there potential risks of regulatory overreach, innovation constraints, or industry burdens?
3. Evaluating Systemic Impacts
   a. Public Trust & Digital Awareness: Do citizens understand & exercise their rights?
   b. Market Readiness & Industry Compliance: Do businesses have the tools to meet obligations?
   c. Regulatory Coherence: Are DPDP rules aligned with existing laws (IT Act, RBI regulations, SEBI data norms, NPD framework)?

This socio-technical perspective ensures that the DPDP Rules are not only legally sound but also practically viable and industry-friendly.

2.4. How This Analysis Informs Recommendations

By combining rights protection analysis with systemic feasibility evaluation, this methodology enables the formulation of balanced policy recommendations that:

1. Enhance individual rights without stifling innovation
2. Ensure robust privacy protections while enabling economic growth
3. Promote business-friendly compliance while maintaining strong enforcement

This dual approach ensures that the DPDP Rules can serve as a global benchmark in data governance, helping India emerge as a leader in privacy, innovation, and inclusive digital growth.

3. Embedding First-Order Rights in the Draft Digital Personal Data Protection Rules, 2025

3.1. Defining First-Order Rights in Data Protection

The foundational principle of data protection is ensuring that individuals, as data principals, retain control over their personal information. First-order rights refer to direct entitlements that empower individuals to access, correct, erase, and control the processing of their personal data. These rights are rooted in constitutional law, international human rights frameworks, and data protection jurisprudence. The Draft Digital Personal Data Protection (DPDP) Rules, 2025, introduce a rights framework, yet they exhibit gaps in enforceability, oversight, and clarity, particularly when compared with international best practices such as the General Data Protection Regulation (GDPR) of the European Union, the California Consumer Privacy Act (CCPA), and Singapore's Personal Data Protection Act (PDPA) (European Parliament & Council of the European Union, 2016; California State Legislature, 2018; Singapore Parliament, 2012).

This chapter evaluates the first-order rights framework in the DPDP Rules, scrutinizing its provisions on fundamental rights (privacy, equality, and freedom of expression), data-specific rights (access, correction, erasure, portability), and context-specific protections (children, vulnerable groups, and public-private interactions). The analysis highlights deficiencies in legislative drafting, regulatory ambiguity, and enforcement challenges, while recommending targeted policy reforms to enhance individual autonomy and safeguard fundamental freedoms.

3.2. Analytical Framework: Categorizing First-Order Rights

3.2.1. Fundamental Rights Rooted in Constitutional and International Law

These rights derive from constitutional guarantees (Article 21 of the Indian Constitution: Right to Privacy), human rights charters (Universal Declaration of Human Rights, ICCPR), and established legal precedents (Justice K.S. Puttaswamy v. Union of India, 2017) (Constitution of India, 1950; United Nations, 1948, 1966; Supreme Court of India, 2017).

1. Right to Privacy: Individuals must have control over their personal data and protection from unwarranted state or corporate intrusion.
2. Right to Equality: The application of data protection measures should be non-discriminatory and inclusive.
3. Right to Freedom of Expression: The framework should not suppress lawful speech, dissent, or digital activism.
4. Right to Life and Dignity: Personal data should not be used to cause physical, psychological, or social harm.

3.2.2. Data-Specific Rights for Digital Autonomy

These rights govern how individuals interact with their data and include:

1. Right to Be Informed: Users must receive clear, accessible, and itemized disclosures on data collection.
2. Right to Transparency: Fiduciaries must disclose processing methods, third-party sharing, and legal bases.
3. Right to Access: Data principals must retrieve their personal data upon request.
4. Right to Correction/Rectification: Users should be able to rectify inaccurate or incomplete data.
5. Right to Erasure (Right to Be Forgotten): Individuals should be able to request deletion of their data under specific conditions.
6. Right to Data Portability: Users should have the ability to transfer their data between services.
7. Right to Restriction of Processing: Individuals must be able to limit how their data is used.
8. Right to Object: Users should be able to refuse data processing that impacts their rights and freedoms.

3.2.3. Context-Specific Rights for Vulnerable Populations

1. Children's Rights: Enhanced protections for minors, including safeguards against behavioral advertising and data exploitation.
2. Rights of Vulnerable Groups: Ensuring digital accessibility, protection from algorithmic bias, and equitable redress mechanisms.
3. Rights in Public-Private Interactions: Preventing government overreach and ensuring independent oversight over state data processing.

3.3. Critical Analysis of First-Order Rights under the DPDP Rules

3.3.1. Right to Privacy: Regulatory Deficiencies and Risks

The DPDP Rules recognize privacy as a guiding principle, yet several draft provisions weaken its enforcement:

1. State Processing Without Consent (Draft Rule 5): The DPDP Rules allow the State to process data without explicit consent for vaguely defined public purposes, lacking a necessity and proportionality test.
2. Consent Manager Discretion (Draft Rule 4): The Data Protection Board (DPBI) holds absolute discretion to suspend consent managers, yet the rules provide no transparency on how such decisions will be justified.

3. Data Minimization and Proportionality: There is no explicit requirement for fiduciaries to collect only the minimum necessary data, creating potential risks of overcollection and function creep.
4. Protecting Data Principals from Manipulation through Dark Patterns: An essential aspect of protecting data principals is ensuring that consent is freely given, informed, and meaningful. The DPDP Rules, 2025, however, do not explicitly address manipulative user interface (UI) patterns, often referred to as dark patterns, which are designed to deceive or coerce individuals into consenting to data collection. These include forced consent through bundled services, misleading opt-ins, or excessive default permissions. International best practices, such as the European Data Protection Board (EDPB) guidelines on dark patterns (2022) and the US Federal Trade Commission (FTC) regulations on deceptive digital design, explicitly prohibit these practices (European Data Protection Board, 2022; Federal Trade Commission, 2022).

Recommendations:

1. Introduce judicial oversight over state data exemptions, mandate explicit proportionality tests, and ensure consent mechanisms are transparent and accountable.
2. A new provision should be introduced under Draft Rule 3, prohibiting deceptive UI/UX practices and ensuring that all consent mechanisms are transparent, fair, and informed. India’s DPDP framework should align with global precedents by:
    a. Explicitly banning misleading UI/UX practices that obscure data processing choices.
    b. Requiring layered or contextual notices that provide real-time, specific explanations about data use.
    c. Mandating periodic consent renewal for long-term data processing, ensuring that individuals have ongoing control over their data.

3.3.2. Right to Equality: Algorithmic Discrimination and Accessibility Barriers

1. Algorithmic Bias in Public Welfare Decisions (Draft Rule 5): The DPDP Rules fail to account for discriminatory outcomes in AI-driven subsidy allocations and social welfare processing. Unregulated AI-driven decision-making can reinforce caste, gender, and socio-economic biases, disproportionately causing disadvantage to marginalized communities. The EU AI Act (2023) and the US Algorithmic Accountability Act (2022) mandate bias audits for high-risk AI applications in public welfare systems (European Union, 2023; U.S. Congress, 2022).
2. Lack of Accessibility Standards (Draft Rules 4 and 7): No requirement for regional language accessibility or alternative formats for persons with disabilities in data breach notifications and consent forms.
3. Children’s Digital Rights (Draft Rule 10): No restrictions on behavioral advertising, algorithmic profiling, or age verification requirements for online platforms targeting minors.

Recommendation:

Mandate bias audits for AI-driven decision-making, ensure algorithmic explainability for state-run services, require regional language accessibility, and ban targeted behavioral advertising for children.

3.3.3. Right to Freedom of Expression: Ensuring Digital Free Speech Protections

1. Suppression Risks in Consent Management (Draft Rule 4): No safeguards prevent consent managers from censoring dissenting voices or restricting access to services based on political or ideological preferences.
2. Social Media and Platform Governance (Draft Rules 4, 9, and 13): The DPDP Rules do not regulate social media content moderation mechanisms, nor do they prevent retaliatory misuse of personal data to suppress speech.
3. Social Media and Platform Governance: Interplay Between DPDP Rules and IT Rules, 2021
    a. The DPDP Rules, 2025, focus on data protection and personal information governance but do not regulate social media content moderation mechanisms. However, social media platforms in India are governed under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021) (Ministry of Electronics and Information Technology [MeitY], 2021), which set transparency and accountability requirements for intermediaries regarding content moderation, user rights, and grievance redressal.
    b. While the IT Rules, 2021, establish mechanisms for content moderation transparency, they do not explicitly address the misuse of personal data for retaliatory actions against users engaging in free speech. There remains a gap in ensuring that social media intermediaries do not exploit user data to suppress speech or enable surveillance-based suppression tactics.

Recommendations:

To ensure comprehensive protections for free expression in the digital ecosystem, a harmonized approach between the DPDP Rules, 2025, and the IT Rules, 2021, is necessary. Specifically:

1. Strengthen data governance protections under the DPDP Rules to prevent the retaliatory misuse of personal data to suppress speech, ensuring that intermediaries cannot weaponize data for political or ideological discrimination.
2. Enhance transparency requirements in content moderation decisions under the IT Rules, 2021, by mandating that social media platforms disclose how personal data is used in enforcement actions, including account suspensions, deplatforming, and shadow bans.
3. Ensure due process protections in platform governance by requiring social media intermediaries to allow users to contest content moderation decisions where personal data

usage played a role in suppression.

By aligning DPDP Rules, 2025, with IT Rules, 2021, India can build a cohesive regulatory framework that safeguards free speech, ensures fair data governance, and enhances transparency in social media governance.

3.3.4. Right to Life and Dignity: Addressing Psychological and Social Harm

1. No Redress for Algorithmic Harm (Draft Rules 6, 8, and 12): Data Fiduciaries and Significant Data Fiduciaries are not required to mitigate social consequences of algorithmic biases that perpetuate discrimination, exclusion, or reputational harm.
2. Inadequate Psychological Safeguards in Data Processing (Draft Rule 13): The grievance redressal framework does not explicitly recognize mental distress caused by data misuse. In cases of profiling-based discrimination, reputational damage due to data leaks, or online harassment enabled by breached personal data, individuals may suffer significant mental distress. Global best practices such as the GDPR's "Right to Effective Remedy" (Article 79) and Singapore's PDPA dispute resolution mechanisms acknowledge non-material harms, including emotional and reputational damage (European Parliament & Council of the European Union, 2016; Singapore Parliament, 2012).

Recommendations:

1. Mandate psychological impact assessments in AI processing, expand grievance redressal mechanisms to include social and mental harm, and ensure fiduciaries are accountable for algorithmic discrimination.
2. Expand Draft Rule 13 to explicitly include psychological harm as a valid grievance category, ensuring comprehensive protection under India's data protection regime. India's DPDP framework should follow global best practices by:
    a. Recognizing psychological harm as a valid basis for grievance redressal.
    b. Allowing claims related to reputational harm, distress caused by algorithmic profiling, or social exclusion due to data misuse.
    c. Mandating fiduciaries to take corrective actions, including public apologies and data restoration efforts, where psychological distress has occurred.

3.4. Strengthening First-Order Rights in India's DPDP Framework

The Draft DPDP Rules lay an important foundation for individual rights in India's digital governance framework, yet several weaknesses remain. These include unchecked state surveillance powers, algorithmic discrimination risks, lack of procedural safeguards, and weak accessibility mandates. By implementing the following reforms, India can align its framework with global best practices.

1. Introduce judicial oversight for state exemptions and national security-related data requests.
2. Mandate fairness audits for AI-driven decision-making, particularly in financial and social welfare allocations.
3. Strengthen accessibility requirements for vulnerable populations and enforce digital inclusivity standards.
4. Recognize psychological harm and mental distress as valid grounds for grievance redressal and data misuse claims.

By integrating these recommendations, India can position itself as a global leader in ethical, inclusive, and privacy-centric data protection frameworks.

4. Strengthening Second-Order Rights for Effective Data Protection

4.1. Introduction: The Structural Foundations of Data Rights

While first-order rights provide individuals with direct control over their personal data, the realization of these rights depends on second-order rights, which serve as institutional and procedural safeguards. These rights ensure that governance mechanisms, oversight structures, and regulatory accountability support the effective implementation of data protection principles. India’s Digital Personal Data Protection (DPDP) Rules, 2025 establish a foundational framework for fair processing, grievance redressal, regulatory transparency, and audit mechanisms, offering a significant opportunity to create a globally aligned and innovation-driven data protection regime.

The conceptual foundation of second-order rights is rooted in legal proceduralism, which asserts that rights must be accompanied by clear institutional safeguards and enforceability mechanisms (Fuller, 1964). This chapter explores the governance and accountability measures within the DPDP Rules through the lens of institutional legitimacy theory, ensuring that regulatory bodies operate in a way that fosters public trust and compliance (Tyler, 2006). By embedding clear procedural guarantees, oversight mechanisms, and participatory policymaking, India can establish itself as a leader in rights-based, inclusive, and effective data governance.

4.2. Analytical Framework: The Role of Second-Order Rights

4.2.1. Governance and Accountability in Data Protection

To ensure that data rights are meaningfully exercised, second-order rights must focus on:

1. Right to Fair Processing: Data fiduciaries must adhere to legally defined fairness principles in processing personal data.
2. Right to Due Process: Individuals must have recourse to legal remedies if their rights are violated.
3. Right to Grievance Redressal: Effective and accessible complaint resolution mechanisms must be in place.
4. Right to Remedies and Compensation: There should be provisions for financial or corrective remedies in cases of data misuse or breaches.

4.2.2. Oversight and Regulatory Transparency

Drawing from administrative law and governance theory, effective data protection frameworks require public accountability and stakeholder participation (Mashaw, 1997):

1. Right to Regulatory Transparency: Data protection authorities must maintain public trust through transparency in enforcement.
2. Right to Participatory Policymaking: Stakeholders should be involved in shaping data protection regulations and governance structures.

4.2.3. Mechanisms for Accountability and Compliance

To maintain institutional integrity and oversight, the following mechanisms are crucial.

1. Right to Audit Information: Ensuring transparency in how fiduciaries process personal data.
2. Right to Impact Assessments: Requiring fiduciaries to evaluate privacy risks in high-risk data processing activities.

4.3. Advancing Governance and Accountability in the DPDP Rules

4.3.1. Ensuring Fair Processing and Due Process Protections

India's Draft DPDP Rules introduce broad principles of fairness but can be strengthened through clearer procedural safeguards:

1. Fair Processing Standards:
   a. Draft Rules 5, and 6: The Draft Rules mandate lawful data processing and require fiduciaries to implement safeguards, yet State instrumentalities are not bound by the same breach notification requirements as private fiduciaries.
   b. Draft Rule 14: The Draft Rules do not require notification of or objection to international data transfers.
2. Due Process in Grievance Resolution (Draft Rule 13): The DPDP establishes a digital-first grievance redressal system, but accessibility challenges may arise for digitally excluded communities.
3. Due Process in Reviewing Decisions of Data Protection Board of India (DPBI) (Draft Rule 21): The Draft Rules empower any person aggrieved by an order or decision of the DPBI to appeal to an Appellate Tribunal established under the Digital Personal Data Protection Act 2023. However, judicial review mechanisms are missing. Judicial review mechanisms ensure independent oversight, procedural fairness, and constitutional accountability in DPBI's decision-making, preventing regulatory overreach, arbitrariness, and potential conflicts of interest while aligning with global best practices in data protection governance.

Recommendations:

1. Ensure State instrumentalities adhere to breach notification requirements.
2. Expand offline grievance redressal mechanisms for digitally marginalized communities.
3. Provide individuals with the right to challenge automated decisions that affect access to

public services.

4. Establish judicial review mechanisms for DPBI decisions, ensuring legal recourse beyond administrative channels.

4.3.2. Strengthening Grievance Redressal Mechanisms

An effective grievance redressal system is essential for maintaining public trust in data governance:

1. Timelines for Grievance Resolution (Draft Rules 12, 19, and 21): The DPDP Rules do not specify response deadlines for fiduciaries or the Data Protection Board of India (DPBI), leading to potential delays.
2. Capacity of DPBI to Manage Complaints: Given the scale of India's digital ecosystem, caseload management mechanisms for DPBI remain unclear.
3. Accessibility for Vulnerable Groups (Draft Rules 13, and 19): Digital-first mechanisms may exclude individuals without consistent internet access, particularly in rural and underserved areas.
4. Transparency in Complaint Resolutions: No requirement exists for DPBI or fiduciaries to publish grievance statistics, limiting public trust in the system's effectiveness.

Recommendations:

1. Set 15-day response timelines for fiduciary-level grievance redressal and 30-45 days for DPBI escalations.
2. Introduce regional DPBI offices to decentralize grievance redressal and enhance accessibility.
3. Mandate DPBI to publish periodic reports on grievance statistics to maintain transparency.
4. Provide offline channels for grievance registration, ensuring inclusivity for non-digital populations.

4.3.3. Introducing Compensation and Non-Monetary Remedies

While the Draft DPDP Rules establish penalties for non-compliant fiduciaries, there are no direct provisions for compensating affected individuals:

1. Penalties for Non-Compliance: While fiduciaries may face penalties, these do not translate into direct financial relief for impacted individuals. Under GDPR, individuals can seek compensation for both material and non-material damage (Article 82), while the California Consumer Privacy Act (CCPA) allows individuals to file class-action lawsuits against non-compliant data processors (European Parliament & Council of the European Union, 2016; California State Legislature, 2018).
2. Lack of Defined Harm Criteria: The Draft Rules do not specify what constitutes harm or the thresholds for claiming compensation.

3. No Mechanism for Non-Monetary Redress: The proposed framework lacks provisions for non-monetary remedies such as apologies, corrective actions, or data restoration.

Recommendations:

Amend Draft Rules 12, and 19 to establish a victim compensation framework, ensuring that affected individuals receive financial or non-monetary remedies.

1. Establish a compensation mechanism for proven cases of data misuse or breaches.
2. Define harm criteria, including financial, reputational, or psychological damage.
3. Allocate a portion of penalties collected by DPBI to redress affected Data Principals.
4. Introduce fast-track small-claims redressal mechanisms for cases involving personal data misuse.
5. Mandate fiduciaries to fund credit monitoring services in financial data breaches to protect users from fraud.
6. Introduce non-monetary remedies such as public apologies or corrective measures.

4.3.4. Enhancing Regulatory Oversight and Transparency

Public accountability of data protection authorities is critical for maintaining trust in the regulatory framework:

1. Lack of Mandatory Public Reporting (Draft Rules 18, and 19): The DPBI is not required to publish decisions, penalties, or enforcement actions.
2. No External Oversight of DPBI Decisions: Unlike global counterparts, DPBI decisions are not subject to independent audit or external review.
3. Absence of Participatory Mechanisms: The current framework lacks public consultation requirements for major policy changes.

Recommendations:

1. Mandate annual reporting by DPBI on complaints, enforcement actions, and compliance trends.
2. Introduce multi-stakeholder advisory bodies to review DPBI's performance.
3. Establish external audit mechanisms for DPBI operations, ensuring regulatory accountability.
4. Require public participation mechanisms in shaping significant policy decisions.

4.4. Strengthening India's Second-Order Rights for a Resilient Digital Ecosystem

India's DPDP Rules offer a strong foundation for regulatory oversight, but key refinements can enhance governance transparency, grievance redressal efficiency, and participatory policymaking. By addressing these areas, India can:

1. Enhance user confidence in data protection mechanisms.
2. Ensure regulatory credibility through structured oversight mechanisms.
3. Align with global best practices while maintaining a unique governance model suited to India's digital economy.

These enhancements will position India as a leader in rights-based, participatory, and innovation-driven data governance.

5. Cross-Cutting Rights in Data Protection: Ensuring Equity, Inclusion, and Technological Justice

5.1. The Need for Inclusive and Equitable Data Protection

As digital governance frameworks evolve, ensuring that data protection laws uphold inclusivity, accessibility, and non-discrimination is essential. Cross-cutting rights intersect multiple domains, ensuring that individuals, regardless of socio-economic status, ability, or cultural identity, can exercise their data protection rights meaningfully. India's Digital Personal Data Protection (DPDP) Rules, 2025 present an opportunity to embed inclusive and ethical data governance into the digital ecosystem.

This chapter applies theoretical perspectives from distributive justice, accessibility law, and algorithmic fairness to analyze linguistic accessibility, disability inclusion, algorithmic fairness, and collective data rights (Rawls, 1971; Stein & Lord, 2017; Binns, 2018). A robust framework must ensure that no individual or community is disproportionately disadvantaged by data governance structures.

5.2. Analytical Framework: Defining Cross-Cutting and Emerging Rights

Cross-cutting rights extend beyond individual entitlements to structural safeguards, ensuring equity and participation. These rights can be categorized into three broad areas:

5.2.1. Cross-Cutting Rights (Inclusivity and Accessibility)

1. Accessibility Rights
    a. Right to Linguistic Accessibility: Ensuring that all individuals, including non-English speakers, can understand and exercise their rights.
    b. Right to Disability Accessibility: Ensuring digital platforms accommodate individuals with disabilities.
2. Equity and Non-Discrimination Rights
    a. Right to Non-Discriminatory Algorithms: Preventing biases in automated decision-making processes.
    b. Right to Equal Opportunity: Ensuring equitable access to digital services and protection mechanisms.
3. Community and Collective Rights
    a. Right to Community Consent: Recognizing collective data governance for indigenous and marginalized groups.
    b. Right to Cultural Preservation: Protecting data linked to cultural identity and heritage from exploitation or erasure.

5.2.2. Emerging Rights (Technology-Driven)

1. AI-Specific Rights
    a. Right Against Profiling: Protection from harmful or opaque algorithmic decisions.
    b. Right to Algorithmic Transparency: Explanations of how algorithms impact outcomes.
2. Blockchain-Specific Rights
    a. Right to Data Immutability Control: Addressing challenges of deleting or modifying data stored on immutable ledgers.
3. Biometric Rights
    a. Right to Biometric Data Protection: Safeguards against misuse of facial recognition or fingerprint data.

5.2.3. Rights by Domain

In addition to the cross-cutting and emerging rights, sector-specific concerns necessitate tailored protections within key industries:

1. Finance: Protection against unfair financial profiling, unauthorized data sharing, and discriminatory credit scoring.
2. Healthcare and Insurance: Ensuring patient data privacy, informed consent for health-related data use, and mitigating AI-driven bias in medical decisions.
3. Education: Safeguarding student data from commercialization, ensuring educational records' privacy, and regulating EdTech data practices.
4. Public Services: Defining proportionality principles for government data collection, preventing overreach in biometric databases, and ensuring transparency in public sector data usage.

5.3. Cross-Cutting Rights: Advancing Inclusivity and Equity in the DPDP Rules

5.3.1. Accessibility and Inclusivity in Data Protection

Theoretical Underpinning: Accessibility as a Foundational Digital Right

Drawing from Amartya Sen’s (2009) capabilities approach, accessibility in data protection is not merely about compliance but about empowering individuals to exercise their rights meaningfully. Without linguistic or disability accessibility, rights become theoretical rather than functional.

Key Issues:

1. Linguistic Barriers (Draft Rule 7): While breach notifications are required, the Rules do not mandate regional language support or accessible formats, disproportionately affecting rural and non-English-speaking populations.
2. Lack of Disability Accessibility (Draft Rules 4, and 10): There are no explicit accessibility obligations for digital platforms, and while verifiable consent mechanisms exist, compliance with global accessibility standards remains undefined.

Recommendations:

1. Mandate regional language translations (i.e. multi-language notification) for data breach alerts and key consent-related documents.
2. Ensure digital platforms comply with Web Content Accessibility Guidelines (WCAG) for accessibility.
3. Require alternate, non-digital channels for grievance redressal, ensuring accessibility for the digitally excluded.

5.3.2. Algorithmic Fairness and Non-Discrimination in AI Decision-Making

Theoretical Underpinning: Fairness in Machine Learning

AI-powered decision-making can reinforce historical biases if not carefully regulated. Theories on fairness in AI stress disparate impact analysis, ensuring that algorithms do not inadvertently disadvantage marginalized groups (Dwork et al., 2012).

Key Issues:

1. Algorithmic Bias (Draft Rules 5, and 12): The Rules do not specify fairness or bias-mitigation measures in AI-driven decision-making, particularly for government services and financial profiling, unlike EU AI Act (2023) which requires fairness testing (European Union, 2024).
2. Opacity in Automated Decisions: GDPR Article 22 provides a right to explanation, while India's DPDP Rules remain silent on this.
3. Lack of Equal Opportunity (Draft Rules 7, and 13): Marginalized groups may face barriers in understanding and exercising data rights, leading to inequitable enforcement.

Recommendations:

1. Require bias audits for AI systems used in high-stakes decision-making (e.g., social benefits, hiring, lending, etc.).
2. Introduce explainability requirements for automated decision-making affecting fundamental rights.
3. Ensure affirmative action for marginalized communities in digital literacy and awareness

initiatives.

4. Require independent AI oversight bodies to ensure compliance.

5.3.3. Strengthening Community and Collective Data Rights

Theoretical Underpinning: The Commons Theory in Data Sovereignty

Elinor Ostrom's Governing the Commons (1990) highlights the need for collective ownership models in resource governance. Data, like natural resources, can be communally owned, especially in indigenous and cultural heritage contexts.

Key Issues:

1. Absence of Collective Consent Mechanisms: Unlike Canada's Indigenous Data Governance Principles (OCAP), India's DPDP framework focuses on individual data rights but does not recognize collective data ownership, crucial for indigenous communities (First Nations Information Governance Centre [FNIGC], 2014). For instance, tribal medicinal knowledge from communities in Jharkhand and Odisha could be accessed by pharmaceutical companies for commercial drug development without requiring consent from the community as a whole, depriving them of both recognition and economic benefits.
2. Cultural Data Exploitation (Draft Rule 15): While data processing is allowed for research and archival purposes, there are no explicit safeguards against misuse of cultural heritage data. This raises risks such as the commercialization of traditional art forms - for example, AI-generated replicas of Madhubani paintings being sold globally without benefiting the original artists. Similarly, tribal oral histories and sacred chants from Northeast India could be digitized and used in commercial media without consultation, eroding cultural ownership and authenticity.

Recommendations:

Expand Draft Rule 15 to introduce a legal framework for collective data ownership and community-governed digital assets.

1. Recognize collective data ownership and governance models ensuring that indigenous groups and marginalized communities have control over data affecting them.
2. Mandate consultation with affected communities before processing cultural, community-linked, and indigenous datasets.
3. Mandate data minimization for cultural and indigenous datasets, preventing commercial exploitation.
4. Introduce ethical processing guidelines for cultural and indigenous datasets.
5. Establish data trusts where communities retain control over their digital assets.

5.4. Emerging Rights in a Technology-Driven Age

5.4.1. Regulating AI Profiling and the Right Against Harmful Automated Decisions

Theoretical Underpinning: The Right Against Profiling in Data Ethics

Drawing from Floridi & Taddeo's (2016) concept of ethical AI, profiling can lead to reinforced stereotypes and oppressive data practices if left unchecked.

Key Issues:

1. No Explicit Ban on High-Risk Profiling (Draft Rules 6, and 10):
   a. Unlike GDPR Article 22, which prohibits AI-based decisions with "legal or similarly significant effects," India's DPDP Rules lack explicit safeguards against AI profiling (European Parliament & Council of the European Union, 2016, Article 22).
   b. The DPDP framework lacks a risk-based AI compliance model, leading to regulatory uncertainty in AI-driven hiring, credit scoring, and social welfare decisions. A tiered risk classification - similar to the EU AI Act - should be introduced to differentiate (European Parliament & Council of the European Union, 2023):
      i. High-Risk AI (Loan approvals, hiring, government profiling): Mandatory bias audits & human oversight.
      ii. Medium-Risk AI (E-commerce recommendations, customer segmentation): Explainability requirements.
      iii. Low-Risk AI (Chatbots, automated notifications): Exempt from stringent compliance.
2. Absence of Algorithmic Transparency (Draft Rules 6, and 12): Data Fiduciaries and Significant Data Fiduciaries are not required to disclose how AI-driven decisions impact individuals.
3. Absence of Human Oversight: Singapore's PDPA mandates human review in automated profiling, whereas India does not (Parliament of Singapore, 2012).

Recommendations:

1. Require explainability measures for automated decision-making affecting employment, credit, and welfare decisions.
2. Establish a right to contest automated decisions, ensuring human oversight in high-impact AI-driven actions.
3. Introduce periodic algorithmic bias audits for Significant Data Fiduciaries.
4. Introduce human-in-the-loop mandates for AI systems making critical decisions.
5. Require data fiduciaries to disclose AI model training data sources.

5.4.2. Addressing Data Immutability Challenges in Blockchain Systems

Theoretical Underpinning: The Paradox of Digital Permanence (Werbach, 2018)

Blockchain's immutability ensures data integrity, but it conflicts with the Right to Erasure ("Right to Be Forgotten"), creating a regulatory dilemma.

Key Issues:

1. Conflicts with Data Deletion Laws (No Explicit Provision in DPDP Rules): Blockchain technology presents a regulatory paradox - while it ensures data integrity and tamper resistance, it conflicts with privacy laws requiring data erasure (Right to Be Forgotten). EU GDPR permits personal data erasure, but blockchain's nature makes data deletions technically unfeasible (European Parliament & Council of the European Union, 2016).
2. No Alternative Compliance Pathways: The French Data Protection Authority recommends cryptographic privacy techniques such as Zero-Knowledge Proofs (ZKPs) and off-chain data storage to balance blockchain compliance with privacy mandates, but India lacks similar provisions (Commission Nationale de l'Informatique et des Libertés [CNIL], 2018).

Recommendations:

Amend Draft Rules 8 and 12 to permit cryptographic obfuscation and ZKP-based compliance models for blockchain networks.

1. Provide alternative compliance models, such as off-chain data storage, and cryptographic obfuscation.
2. Establish sectoral guidelines for blockchain-based processing, ensuring clarity on compliance with privacy rights.
3. Establish technical standards for privacy-preserving blockchain models (e.g., zero-knowledge proofs).

5.4.3. Strengthening Biometric Data Protections

Theoretical Underpinning: Biometric Data as a Unique Identifier

Biometric data is permanent and irreplaceable, making unauthorized collection and processing highly sensitive. Surveillance capitalism warns against unchecked biometric data aggregation (Ratha et al., 2018; Zuboff, 2019).

Key Issues:

1. Lack of a Sensitive Data Classification (Draft Rule 4): India's DPDP Rules do not differentiate biometric data from general personal data, leaving it vulnerable to mass surveillance abuses. Unlike the EU AI Act, which bans real-time biometric tracking in public spaces, India's framework lacks clear restrictions on facial recognition technology (FRT) (European

Union, 2024). GDPR (Recital 51) classifies biometric data as sensitive, while India does not (General Data Protection Regulation [GDPR], 2016, Recital 51).

2. Mass Surveillance Risks: China's Social Credit System leverages facial recognition; India lacks biometric surveillance regulations (Creemers, 2018; Liang et al., 2018).

Recommendations:

Amend Draft Rules 4 and 8 to establish strict governance controls on biometric authentication.

1. Define biometric data as sensitive personal data, requiring explicit, informed consent for collection and storage.
2. Establish governance mechanisms for facial recognition and biometric authentication, ensuring ethical deployment and accountability.
    a. Limit real-time biometric tracking in non-law enforcement contexts.
    b. Establish strict necessity tests for facial recognition deployments.
3. Mandate privacy-enhancing technologies (e.g., federated learning models) for biometric storage, such as encryption and federated learning models.

5.5. Ensuring Domain-Specific Data Protections

Theoretical Underpinning: Contextual Privacy Theory

Privacy expectations vary by sector, necessitating domain-specific protections in finance, healthcare, education, and public services (Nissenbaum, 2010).

Key Issues:

1. **Finance - No Explicit Safeguards Against Credit Scoring Bias:** Unlike the US Fair Credit Reporting Act (FCRA), India lacks consumer protection laws for algorithmic credit scoring (Fair Credit Reporting Act, 1970).
2. **Healthcare - No Sector-Specific Security Standards:** HIPAA (US) mandates stronger health data protection, while India's DPDP framework does not (Health Insurance Portability and Accountability Act [HIPAA], 1996).
3. **Education - Lack of EdTech Data Safeguards:** COPPA (US) restricts EdTech companies from monetizing student data, but India has no such provisions (Children's Online Privacy Protection Act [COPPA], 1998).
4. **Public Services - Government Data Processing Exemptions:** GDPR Article 23 limits state data processing exemptions, whereas India's DPDP framework has broad exemptions for government entities (General Data Protection Regulation [GDPR], 2016, Article 23).

Recommendations:

1. Finance: Mandate explainability in AI-driven credit scoring models.
2. Healthcare: Enforce encryption and anonymization mandates for medical records.
3. Education: Prohibit EdTech companies from monetizing student data.
4. Public Services: Introduce proportionality tests for government data collection exemptions.

5.6. Strengthening India’s Cross-Cutting and Emerging Rights Framework

The Digital Personal Data Protection (DPDP) Rules, 2025 lay the foundation for inclusive, ethical, and future-focused digital governance. However, to ensure robust protections across diverse populations, emerging technologies, and key sectors, targeted refinements are required. Strengthening cross-cutting rights, emerging technology regulations, and domain-specific safeguards will help India balance innovation with accountability, equity, and security.

By implementing the proposed measures, India can:

1. Ensure digital accessibility and inclusion by embedding linguistic and disability-friendly mechanisms within data governance.
2. Enhance algorithmic fairness and transparency by mandating explainability, bias audits, and safeguards against profiling in AI-driven decision-making.
3. Recognize collective and cultural data rights, empowering indigenous communities and ensuring ethical data governance in research and archival processes.
4. Address technological challenges in blockchain and biometrics, ensuring compliance with global best practices on data erasure, consent, and security.
5. Establish sectoral protections for finance, healthcare, education, and public services, ensuring context-sensitive regulatory measures to prevent discrimination, misuse, and exploitation.

India stands at a pivotal moment to lead the global discourse on equitable, inclusive, and ethical data protection. By embedding strong accessibility frameworks, AI and blockchain accountability measures, and industry-specific safeguards, India can set a precedent for rights-driven digital governance - one that promotes trust, innovation, and economic growth while protecting individual and community rights in the digital age.

6. Socio-Technical Systems (STS) Analysis: Systemic Impact of Draft DPDP Rules

6.1. Conceptualizing the DPDP Ecosystem through the STS Lens

6.1.1. Theoretical Foundations of Socio-Technical Systems in Digital Governance

The Socio-Technical Systems (STS) framework provides a lens through which the interplay between human actors, institutional structures, and technological infrastructures can be analyzed in regulatory ecosystems. The STS perspective, first articulated by Trist and Bamforth (1951) and later expanded by Bijker & Law (1992), suggests that technological artifacts are not merely neutral tools but are embedded within social, economic, and political contexts (Trist & Bamforth, 1951; Bijker & Law, 1992).

In the context of data protection, the DPDP Rules, 2025, function within a complex STS ecosystem where compliance is not only a technical challenge (encryption, security protocols, algorithmic governance) but also an institutional and social challenge (enforcement capacity, market readiness, public awareness).

From an STS perspective, three core interdependencies shape India's data protection framework:

1. Regulatory Interplay: How the DPDP framework interfaces with existing legal instruments (e.g., IT Act, RBI, SEBI, and sectoral data laws).
2. Technological Constraints: The feasibility of compliance for different stakeholders, particularly MSMEs, startups, and state agencies.
3. Social Adaptability: Whether the rights and obligations outlined in DPDP can be effectively exercised by individuals with varying levels of digital literacy and access to grievance mechanisms.

These interdependencies necessitate an STS-based evaluation to ensure that policy formulation aligns with real-world implementation.

6.1.2. DPDP as a Socio-Technical System: Interactions between Law, Technology, and Human Actors

Applying STS theory to the DPDP framework, we observe a multi-layered governance model in which:

1. Legal Norms (privacy rights, consent, fiduciary obligations) define the principles.
2. Technological Systems (data infrastructures, encryption, automated compliance) enforce the principles.

3. Human Actors (regulators, fiduciaries, citizens) interpret, challenge, and comply with these principles.

Unlike traditional legal frameworks, data protection laws are inherently STS-driven, as compliance hinges not only on regulatory willpower but also on technical feasibility and societal adoption. For example, requiring algorithmic explainability is meaningful only if:

1. Firms have the technological ability to implement transparency.
2. Regulators have the institutional capacity to audit AI-driven systems.
3. Citizens have adequate digital literacy to contest AI-based decisions.

Thus, the DPDP ecosystem cannot be evaluated solely as a legal instrument - it must be assessed through STS methodologies to understand its functional dynamics.

6.1.3. Comparative Perspective: STS Applications in Global Data Protection Regimes

STS frameworks have been instrumental in shaping data protection laws across jurisdictions. A comparative analysis reveals:

1. EU General Data Protection Regulation (GDPR): The GDPR is a classic STS-informed framework, incorporating human-centric governance (Data Protection Impact Assessments, AI transparency requirements) while recognizing technological and market constraints (grace periods for SME compliance) (European Parliament & Council of the European Union, 2016).
2. Singapore’s Personal Data Protection Act (PDPA): Singapore integrates tech-driven compliance models such as privacy-by-design frameworks with institutional mechanisms like the Data Protection Trustmark, which balances business interests with regulatory enforcement (Singapore Parliament, 2012).
3. California Consumer Privacy Act (CCPA): The CCPA adopts a market-driven STS approach, enabling consumer opt-outs while allowing businesses to comply through data valuation models (e.g., differential pricing for consent-based data sharing) (California State Legislature, 2018).

In contrast, India’s DPDP framework lacks a clear STS-informed enforcement strategy, particularly in balancing technological constraints with regulatory mandates. Key STS lessons from these jurisdictions include:

1. Institutional Readiness Matters: GDPR and PDPA have sectoral regulatory enforcers, whereas India's DPBI is still evolving.
2. Technological Incentives Improve Compliance: The Singapore model integrates data protection certifications, making compliance a market differentiator.

3. Public Awareness Enhances Effectiveness: The CCPA model thrives on consumer awareness, which is still underdeveloped in India's DPDP framework.

6.1.4. Key Takeaways for India's DPDP Framework

Applying STS analysis, three challenges emerge in India's DPDP implementation:

1. Fragmented Regulatory Landscape: Lack of clarity on sectoral interplay (RBI, SEBI, IRDAI) with DPDP.
2. Feasibility of Compliance for MSMEs: Smaller firms lack in-house legal/technical teams, making compliance resource-intensive.
3. Public Trust & Digital Literacy Gaps: Without awareness and usability mechanisms, data principals may not exercise their rights effectively.

6.2. Mapping the Socio-Technical Actors in India's DPDP Ecosystem

6.2.1. Understanding the Multi-Stakeholder Data Protection Ecosystem

The DPDP framework operates within a complex socio-technical network where multiple stakeholders interact to enforce, comply with, and contest data protection regulations. Unlike traditional legal systems, which rely primarily on hierarchical enforcement, the effectiveness of DPDP depends on a distributed governance model - where regulatory institutions, businesses, intermediaries, and individuals collectively shape compliance and enforcement.

In STS theory, Actor-Network Theory (ANT) posits that regulatory success depends not only on legal mandates but on the strength of networks that implement and uphold these mandates (Latour, 2005). In the DPDP ecosystem, this includes:

1. Regulatory Bodies (Government & DPBI)
2. Data Fiduciaries (Large & Small Enterprises)
3. Consent Managers & Data Processors (Compliance Intermediaries)
4. Data Principals (Citizens, Communities, and Vulnerable Groups)

Each of these actors plays a distinct role in the socio-technical system of data governance.

6.2.2. Key Actors and Their Interactions in the DPDP Ecosystem

1. Regulatory Bodies: MeitY, DPBI, and Sectoral Regulators

1. Role: Set policy, enforce compliance, and resolve disputes.
2. Challenges: Institutional capacity constraints, sectoral overlap, and regulatory clarity.
3. STS Perspective: The Data Protection Board of India (DPBI), as the primary enforcement agency, must operate as a hybrid regulatory body, balancing technical oversight (data audits, security compliance) with legal adjudication (grievance redressal, penalties).

4. Comparison: GDPR's Data Protection Authorities (DPAs) are independently funded, ensuring robust oversight. India's DPBI, however, lacks clear financial and structural autonomy, potentially affecting enforcement effectiveness.
5. Key Concern: The DPBI lacks institutional capacity to handle mass-scale grievances, raising concerns about backlogs and regulatory inefficiencies.
6. Recommendation: Introduce decentralized DPBI offices across states to handle region-specific grievances, ensuring faster adjudication.

2. Data Fiduciaries: Large Tech Firms, MSMEs, and Public Sector Entities

1. Role: Collect, store, and process personal data while ensuring compliance.
2. Challenges: Compliance burdens, cybersecurity risks, and balancing innovation with regulation.
3. STS Perspective: Large platforms (Google, Meta, Amazon) have advanced compliance teams, but MSMEs, health-tech startups, and EdTech firms lack the same resources.
4. Comparison: In the EU, GDPR compliance is tiered - small businesses have fewer obligations. India's DPDP lacks sectoral exemptions, which could disproportionately burden startups and MSMEs.
5. Key Concern: Micro and small enterprises face compliance costs that may limit innovation or push firms into informal/unregulated spaces.
6. Recommendation: Introduce a compliance assistance program for MSMEs, providing template privacy policies, low-cost audit tools, and advisory services.
7. Additionally, India's Digital Public Infrastructure (DPI) - including Aadhaar, UPI, DigiLocker, and ONDC - is deeply embedded in data processing ecosystems. The DPDP framework must incorporate DPI compliance structures to:
    a. Use DigiLocker for user-controlled consent dashboards, enabling individuals to view, modify, or revoke permissions.
    b. Ensure ONDC interoperability safeguards, preventing unauthorized data aggregation across e-commerce platforms.
    c. Align with UPI-based data governance, ensuring that financial and identity-based transactions comply with privacy-by-design principles.

3. Consent Managers & Data Processors: The Compliance Intermediaries

1. Role: Facilitate consent transactions between users and fiduciaries.
2. Challenges: Lack of regulatory clarity, risk of monopolization.
3. STS Perspective: Consent managers act as trust intermediaries, governing the flow of permissions between individuals and platforms.
4. Comparison: Singapore's Data Protection Trustmark (DPTM) program certifies intermediaries, ensuring standardized compliance mechanisms. India lacks a comparable accreditation system (Infocomm Media Development Authority [IMDA], n.d.).

5. Key Concern: The DPDP does not specify minimum security standards for consent managers, creating risks of data misuse and non-compliance.
6. Recommendation: Establish a "DPBI Certified Consent Manager" program, ensuring that only verified entities can operate consent facilitation platforms.

4. Data Principals: Citizens, Communities, and Vulnerable Groups

1. Role: Exercise data rights (access, correction, erasure, portability).
2. Challenges: Digital literacy gaps, limited access to grievance redressal.
3. STS Perspective: Users do not engage with legal frameworks in isolation - they require technological support systems (user-friendly interfaces, notification systems, digital literacy aids).
4. Comparison: The CCPA (California) mandates user-friendly privacy dashboards, whereas India’s DPDP framework relies on written consent mechanisms, which may be inaccessible to low-literacy populations (California State Legislature, 2018).
5. Key Concern: Vulnerable groups (rural users, elderly, disabled individuals) lack support structures to navigate complex data rights processes.
6. Recommendation: Implement community-based digital literacy programs and develop audio/video explainer tools in regional languages to make data rights accessible to all citizens.

6.3. Implementation Barriers and Practical Constraints

6.3.1. Understanding the Implementation Challenges of the DPDP Rules

While the DPDP Rules, 2025 establish a legal framework for digital governance, their real-world effectiveness depends on how well various stakeholders can comply with, enforce, and navigate the regulatory landscape. This section applies STS theory to examine whether compliance is feasible for businesses, regulators, and individuals within India's socio-technical environment.

Drawing from Regulatory Compliance Theory, and Institutional Capacity Frameworks, this section highlights three major constraints (Baldwin, 2012; North, 1990):

1. Barriers for Data Fiduciaries (Businesses & MSMEs)
2. Capacity Constraints for Regulators (DPBI & Government)
3. Practical Limitations for Individuals (Data Principals)

1. Compliance Barriers for Data Fiduciaries

Key Question: Are the compliance obligations under DPDP feasible for startups, MSMEs, and large enterprises?

Challenges Identified:

1. High Compliance Burden on MSMEs & Startups:
    a. The DPDP mandates data protection audits, impact assessments, and breach notifications, but small businesses may lack legal or technical expertise to fulfill these obligations.
    b. Comparison: Under GDPR, compliance requirements are tiered - smaller firms face fewer obligations, unlike India's DPDP, which imposes uniform obligations (European Parliament & Council of the European Union, 2016).
2. Unclear Cross-Border Data Transfer Obligations
    a. The DPDP Rules allow international data transfers but do not specify security or localization standards.
    b. Impact: This creates uncertainty for Indian SaaS firms and fintechs operating in cross-border digital markets.
3. Limited Resources for Cybersecurity Compliance
    a. Many health-tech, fintech, and EdTech startups lack resources to conduct regular security audits and encryption safeguards.
    b. Impact: MSMEs risk non-compliance and penalties due to inadequate data protection infrastructure.

Recommendations:

1. Introduce Tiered Compliance Obligations
    a. Large tech firms: Full compliance (impact assessments, AI audits).
    b. MSMEs/startups: Simplified self-assessment checklists to reduce compliance burden.
2. Clarify Data Localization & Cross-Border Transfers
    a. Define sector-specific transfer obligations (e.g., stricter for health & financial data, flexible for e-commerce & SaaS firms).
3. Establish a Compliance Assistance Program
    a. Provide low-cost legal templates, cybersecurity toolkits, and advisory support for startups and MSMEs.

2. Regulatory Capacity Constraints

Key Question: Does the Data Protection Board of India (DPBI) have the institutional capacity to oversee and enforce the DPDP framework effectively?

Challenges Identified:

1. Institutional Gaps in DPBI's Enforcement Authority
    a. The DPBI lacks independent funding and sectoral enforcement capacity.
    b. Impact: This may lead to delayed adjudications and ineffective enforcement.
2. Potential Backlogs in Grievance Redressal
    a. The DPBI is a centralized authority but may face a high volume of complaints.

   b. Impact: Regulatory bottlenecks may delay resolutions, harming consumer trust.
3. Overlapping Jurisdictions with Existing Regulators
   a. RBI, SEBI, and IRDAI already regulate data in financial, securities, and insurance sectors.
   b. Impact: Unclear division of responsibilities between DPBI and these regulators may create legal conflicts.

Recommendations:

1. Strengthen DPBI's Institutional Capacity
   a. Ensure independent funding & staffing autonomy for DPBI.
   b. Introduce regional DPBI offices to decentralize compliance enforcement.
2. Create a Fast-Track Grievance Resolution Mechanism
   a. Establish sectoral grievance cells (e.g., fintech, health data, AI-driven decisions) to streamline case management.
3. Define Regulatory Overlap Rules
   a. Clarify sectoral boundaries between DPBI, RBI, SEBI, and IRDAI through inter-regulator coordination mechanisms.
4. Specifically, while DPBI is positioned as the primary data protection authority, it currently lacks institutional independence and sectoral enforcement capacity. Without financial autonomy, regional regulatory presence, and inter-agency coordination, DPBI risks becoming a bottleneck for compliance enforcement. A phased institutional strengthening plan is essential:
   a. Year 1: Grant DPBI financial independence to reduce reliance on executive directives.
   b. Year 2: Establish sectoral enforcement units (Fintech, AI, Health, E-commerce) for specialized data oversight.
   c. Year 3: Transition DPBI into a fully independent statutory authority, with parliamentary oversight for regulatory accountability.

3. Accessibility & Awareness Barriers for Individuals

Key Question: Can individuals understand and effectively exercise their data rights under the DPDP framework?

Challenges Identified:

1. Low Digital & Legal Literacy
   a. Many individuals do not understand how to access, correct, or delete their data.
   b. Impact: Rights remain theoretical rather than practical.
2. Lack of Multilingual & Accessible Communication
   a. DPDP notices are not required to be available in regional languages or accessible formats.

   b. Impact: Rural users and persons with disabilities may struggle to access their rights.

3. Difficulties in Filing Data Grievances
   a. Grievance redressal requires digital-first access, but many Indians lack reliable internet.
   b. Impact: This creates barriers for the elderly, rural populations, and digitally marginalized groups.

Recommendations:

1. Launch Nationwide Data Rights Awareness Programs
   a. Run digital literacy campaigns (TV, radio, print, vernacular media) to educate citizens about their rights.
2. Mandate Multilingual & Accessible DPDP Notices
   a. Require regional language translations, Braille, and audio formats for key consent & data breach notifications.
3. Provide Offline & Assisted Grievance Filing
   a. Establish physical grievance centers at post offices, Common Service Centers (CSCs), and panchayat offices for rural users.

6.3.2. Assessing Institutional & Market Readiness for DPDP Compliance

The success of any data protection law depends not only on its legal structure but also on the institutional and market readiness to implement its provisions effectively. The Draft Digital Personal Data Protection (DPDP) Rules, 2025 require businesses, regulators, and citizens to adopt new compliance mechanisms, cybersecurity safeguards, and rights-based enforcement practices.

Using Institutional Readiness Theory and Regulatory Adaptation Models, this section evaluates (Tolbert & Zucker, 1996; Baldwin, 2012):

1. Public Trust & Awareness: Do citizens understand and exercise their data rights?
2. Business Preparedness: Are Indian industries equipped for DPDP compliance?
3. Regulatory Alignment: Does DPDP integrate well with existing financial, cybersecurity, and digital economy laws?

1. Public Trust & Digital Awareness

Key Question: Do citizens understand their data rights under DPDP, and do they trust the data protection ecosystem?

Challenges Identified:

1. Low Awareness of Data Protection Rights
   a. Internet users may be unaware of their rights under data protection laws.

   b. Impact: Citizens may not file grievances or exercise their rights, limiting the effectiveness of DPDP protections.
2. Distrust in Data Fiduciaries
   a. Users may lack confidence in platforms' ability to handle their data securely.
   b. Global Insight: In the EU, GDPR enforcement led to increased public trust due to high-profile penalties against tech firms - India lacks similar deterrence mechanisms (European Parliament & Council of the European Union, 2016).
3. Challenges for Vulnerable Groups
   a. Women, rural populations, and low-income users may face higher risks of data misuse but have fewer resources to seek redress.
   b. Example: A rural SHG (Self-Help Group) may be unaware that financial data collected for microcredit schemes can be processed or shared without clear consent.

Recommendations:

1. Run Large-Scale Data Literacy Campaigns
   a. Use TV, radio, and vernacular media to explain digital rights in regional languages.
   b. Introduce a DPDP Helpline for grievance redressal assistance.
2. Strengthen User Trust via Transparency Mandates
   a. Require periodic privacy audits to be publicly available, increasing accountability.
3. Develop Data Rights Programs for Women & Marginalized Groups
   a. Partner with women's organizations, rural NGOs, and financial literacy groups to empower vulnerable populations to assert their digital rights.

2. Business Preparedness & Compliance Costs

Key Question: Are Indian fintech, health-tech, e-commerce, and MSME industries ready for DPDP implementation?

Challenges Identified:

1. Lack of Readiness Among MSMEs
   a. Micro, Small, and Medium Enterprises (MSMEs) are pivotal to India's economy, comprising approximately 59.3 million to 63 million units, and contributing around 30% to the nation's GDP. Notably, over 99% of these enterprises are classified as micro-enterprises, reflecting their small-scale operations (Press Information Bureau [PIB], 2025; Forbes Advisor, 2024; International Finance Corporation [IFC], 2024). Due to their limited scale and resources, many MSMEs often lack dedicated legal and compliance teams. This absence can lead to challenges in navigating complex regulatory landscapes, potentially resulting in non-compliance and associated penalties.

   b. Impact: MSMEs struggle with implementing consent, grievance mechanisms, and data audits.

2. Unclear AI & Automated Processing Rules
   a. Fintechs, health-tech firms, and e-commerce platforms rely on AI-powered decision-making.
   b. Challenge: DPDP does not specify AI transparency obligations, making compliance uncertain for AI-driven platforms.
3. Sector-Specific Gaps
   a. Fintech: DPDP does not clarify credit scoring or financial profiling safeguards.
      i. DPDP rules must explicitly align with India's fintech regulations (RBI's digital lending norms, SEBI's AI-driven trading guidelines) to avoid compliance conflicts. Establishing a Fintech & AI Regulatory Coordination Unit within DPBI would ensure harmonization of AI profiling rules across financial services (Reserve Bank of India [RBI], 2022; Securities and Exchange Board of India [SEBI], 2023).
   b. Healthcare: No sector-specific security norms for patient data.
   c. E-Commerce: No restrictions on behavioral tracking & targeted advertising.

Recommendations:

1. Introduce MSME Compliance Toolkits
   a. Develop simplified compliance templates for small businesses, reducing compliance burden.
2. Clarify AI Governance Under DPDP
   a. Introduce sector-specific guidance on AI decision-making (e.g., bias audits for AI-based lending decisions).
3. Establish Industry-Specific DPDP Standards
   a. Define fintech, health-tech, and e-commerce compliance obligations separately, ensuring industry alignment.

3. Regulatory Coordination & Legal Alignment

Key Question: How well does DPDP align with India's existing legal and regulatory ecosystem?

Challenges Identified:

1. Overlapping Jurisdiction with RBI, SEBI, IRDAI
   a. RBI already regulates financial data security, while SEBI governs investment data privacy.
   b. Impact: Unclear jurisdictional boundaries between DPBI and financial regulators may cause compliance conflicts.
2. Lack of Clarity on Cybersecurity Integration

a. India's CERT-In guidelines (2022) require data breach reporting - DPDP introduces overlapping obligations (CERT-In, 2022).
b. Impact: Companies may face dual reporting requirements, increasing compliance complexity.

3. Integration with India's AI & Digital Economy Policies
    a. DPDP does not define how it aligns with India's AI governance framework.
    b. Impact: Conflicting norms may emerge in automated decision-making, biometric surveillance, and fintech AI scoring.

Recommendations:

1. Develop an Integrated Data Protection Coordination Mechanism
    a. Establish an Inter-Regulator Committee to align DPBI with RBI, SEBI, IRDAI, and CERT-In.
2. Clarify DPDP's Role in Cybersecurity Governance
    a. Define a clear distinction between DPBI's mandate & CERT-In's cybersecurity oversight.
3. Align DPDP with India's AI & Fintech Regulations
    a. Mandate that AI-based financial & health-tech decisions comply with DPDP's data fairness principles.

6.3.3. Balancing Regulatory Oversight with Innovation-Friendly Governance

The Digital Personal Data Protection (DPDP) Rules, 2025 seek to strengthen data rights and accountability, but they must also foster innovation in India's growing digital economy. Striking the right balance between regulatory oversight and economic growth is critical to ensuring that businesses comply without excessive burdens that discourage technological advancement.

Using frameworks such as Regulatory Sandboxing, and Risk-Proportionate Regulation, this section explores (OECD, 2020; Baldwin, 2012):

1. Compliance Burdens vs. Economic Competitiveness: Are DPDP obligations practical for India's digital economy?
2. Avoiding Conflicting Norms: Does DPDP align with India's fintech, AI, and cybersecurity regulations?
3. Minimizing Bureaucratic Inefficiencies: Does DPDP promote ease of doing business while ensuring data security?

1. Compliance Burdens vs. Economic Competitiveness

Key Question: Does DPDP impose excessive compliance burdens on startups, MSMEs, and digital innovators?

Challenges Identified:

1. Disproportionate Compliance Costs for MSMEs & Startups
    a. While large enterprises can afford dedicated compliance teams, MSMEs and startups struggle with high compliance costs.
    b. Example: A small health-tech startup using patient data for AI-driven diagnosis may find DPDP compliance costly, limiting its ability to scale.
2. Over-Regulation Could Deter Investment
    a. Strict data localization requirements and uncertainty around AI-based decision-making rules may discourage foreign investors and startups.
    b. Example: Indian fintech startups using AI-driven credit scoring may struggle if DPDP introduces unclear AI profiling restrictions, leading to investor hesitation.
3. Sector-Specific Regulatory Uncertainty
    a. Fintechs, AI-driven platforms, and e-commerce players require clear sectoral guidelines.
    b. Example: E-commerce platforms may be impacted by DPDP's restrictions on targeted advertising, reducing personalization and consumer engagement.

Recommendations:

1. Implement a Tiered Compliance Model for MSMEs
    a. Allow small startups & MSMEs to adopt scaled-down compliance frameworks while ensuring fundamental privacy protections.
2. Introduce Regulatory Sandboxes for AI & Fintech Innovation
    a. Permit fintechs, AI startups, and digital health firms to experiment with compliant data processing in controlled environments.
3. Provide Clear, Industry-Specific Compliance Roadmaps
    a. Develop DPDP implementation guidelines for fintech, AI, health-tech, and e-commerce.

2. Avoiding Conflicting Norms Across Indian Regulations

Key Question: Does DPDP align well with India's AI, fintech, and cybersecurity regulations, or does it create conflicts and redundancies?

Challenges Identified:

1. Overlap with RBI, SEBI, and CERT-In Guidelines
    a. Fintech data protection is already regulated under RBI's digital lending guidelines.
    b. CERT-In (2022) cybersecurity guidelines require breach notifications, overlapping with DPDP (CERT-In, 2022).
    c. DPDP's AI transparency and financial data governance should be harmonized with RBI's fintech policies and SEBI's financial AI guidelines to ensure regulatory clarity

for AI-driven credit scoring and digital lending (Reserve Bank of India [RBI], 2022; Securities and Exchange Board of India [SEBI], 2023).

2. Lack of Clarity on AI-Driven Decision-Making
    a. India's AI policy is evolving, but DPDP does not clarify:
        i. Are AI credit scoring models considered "profiling"?
        ii. Do consumers have a "right to explanation" for AI-driven decisions?
    b. Establishing a risk-tiered AI governance framework is critical for balancing innovation with compliance. AI-powered credit scoring, hiring models, and state-run AI welfare distributions should be classified as "High-Risk AI", mandating explainability, bias audits, and contestability.
3. Data Localization vs. Global Cloud Infrastructure
    a. DPDP permits cross-border data flows under conditions yet to be defined.
    b. Impact: Lack of clarity could disrupt businesses relying on global cloud computing.

Recommendations:

1. Establish Inter-Regulatory Coordination Between DPBI, RBI & SEBI
    a. Ensure DPDP rules complement fintech & cybersecurity regulations to avoid duplicate compliance efforts.
2. Define AI Transparency Obligations Under DPDP
    a. Require "explainability" standards for AI-based profiling in financial and hiring decisions.
3. Clarify Cross-Border Data Transfer Requirements
    a. Define clear conditions for permissible data flows, aligning DPDP with global cloud computing best practices.

3. Mitigating Bureaucratic Inefficiencies in DPDP Implementation

Key Question: Can DPDP be enforced efficiently and predictably without creating administrative bottlenecks?

Challenges Identified:

1. Delays in Grievance Redressal & DPBI Enforcement
    a. Example: If DPBI takes months to adjudicate data complaints, businesses may face uncertainty, and citizens may lose trust in the system.
2. Overloading Regulatory Infrastructure
    a. DPBI may struggle with enforcement due to a high volume of complaints and limited capacity.
    b. Example: If thousands of complaints arise without sufficient staff, DPBI could become backlogged.
3. Potential for Regulatory Capture

   a. Lack of independent oversight may lead to industry influence over enforcement, reducing regulatory effectiveness.

Recommendations:

1. Develop a Time-Bound Complaint Resolution Framework
   a. Set maximum response timelines (e.g., 30 days for fiduciaries, 60 days for DPBI rulings).
2. Strengthen DPBI's Institutional Capacity
   a. Allocate higher budgets and expert staff to handle regulatory enforcement efficiently.
3. Ensure External Oversight for DPBI Decisions
   a. Establish independent review panels to prevent regulatory capture.
4. DPI Integration within DPDP Enforcement
   a. DPI integration within DPDP enforcement can streamline compliance for businesses while enhancing transparency for users. Leveraging DigiLocker for real-time privacy dashboards and ONDC for structured consent exchange can minimize regulatory burdens for fintech, health-tech, and e-commerce platforms.

6.4. Strengthening the DPDP Framework Using the STS Lens

A successful Digital Personal Data Protection (DPDP) framework must be legally robust, practically implementable, and industry-friendly. While the DPDP Rules, 2025 lay a strong foundation, enhancements are necessary to address regulatory capacity gaps, business compliance challenges, and alignment with global best practices.

This section provides strategic recommendations to:

1. Enhance Institutional Capacity: Strengthening DPBI's enforcement mechanisms.
2. Facilitate MSME & Startup Compliance: Reducing compliance burdens for smaller enterprises.
3. Align with Global Best Practices: Learning from EU GDPR, Singapore PDPA, and US CCPA.

By embedding these socio-technical refinements, India can establish a resilient, innovation-driven, and rights-protective data governance model.

7. Conclusion: India's Roadmap for Global Leadership in Data Protection and AI Governance

India's Digital Personal Data Protection (DPDP) Rules, 2025 present a historic opportunity to create an inclusive, future-ready, and globally influential data protection framework. By integrating a rights-based approach with a socio-technical systems (STS) analysis, this report has highlighted key gaps, systemic challenges, and strategic solutions necessary to enhance regulatory capacity, foster digital equity, and position India as a leader in AI and data governance.

To realize this vision, India must balance innovation and accountability, ensuring business-friendly implementation while embedding strong citizen protections. The following roadmap outlines a realistic yet ambitious strategy to enhance governance, accelerate AI oversight, and secure India's leadership in global digital policy.

Short-Term (0-2 Years): Strengthening Foundational Implementation

1. **Institutional Independence for DPBI:** Transition DPBI into an independent regulatory authority within two years, ensuring financial autonomy by Year 1 and sectoral enforcement divisions by Year 3.
2. **Accessibility & Linguistic Compliance:** Ensure regional language notifications and disability-friendly grievance redressal mechanisms within 24 months.
3. **AI Bias & Profiling Redressal Pilot:** Launch AI auditing sandboxes to assess fairness in loan approvals, welfare allocation, and hiring by Year 2.
4. **Data Protection Toolkits for MSMEs & Startups:** Introduce sector-specific compliance guidelines to ease regulatory burdens on small enterprises.
5. **Cross-Border Data Transfer Readiness:** Establish a framework for regional data-sharing under G20, BRICS, or IPEF negotiations.

Medium-Term (2-5 Years): Scaling Regulatory Alignment & AI Governance

1. **AI Oversight & Explainability Regulations:** Operationalize AI risk classification by Year 3, ensuring mandatory explainability & bias audits for high-risk AI applications.
2. **Privacy-Preserving Technologies (PETs) as Industry Standard:** Mandate adoption of differential privacy, encryption standards, and federated learning by Year 4.
3. **Regulatory Integration with Fintech, Cybersecurity, and HealthTech:** Align DPDP compliance with RBI's fintech rules, SEBI's data frameworks, and the National Digital Health Mission.
4. **Cross-Border Data Transfer Agreements by Year 3:** Initiate bilateral and regional negotiations for data adequacy partnerships with ASEAN, the EU, and key trade partners.

Long-Term (5+ Years): Global Leadership & Exporting India’s Data Governance Model

1. **Global South Digital Sovereignty Consortium by Year 5:** Position India as a leader in digital sovereignty for emerging economies, promoting context-driven AI & data protection models. Lead multilateral cooperation in privacy-preserving AI and ethical data governance.
2. **India’s “Responsible AI for Bharat” Framework by Year 5:** Develop a global benchmark for AI ethics & governance tailored for diverse, high-population economies. Promote an inclusive AI governance model for emerging economies, focusing on fairness, accessibility, and algorithmic transparency.
3. **Establish India’s Global Digital Trust Model:** Promote India’s data protection regime as a standard for fair, accessible, and innovation-driven digital governance.
4. **Diplomatic Leadership in AI & Data Governance:** India should leverage its G20 Presidency, BRICS engagement, and partnerships with the African Union and ASEAN to champion equitable AI & data policy frameworks.

Positioning India as a Global Leader

By following this roadmap, India can:

1. Ensure digital inclusion and accessibility by embedding linguistic and disability-friendly mechanisms within data governance.
2. Enhance algorithmic fairness and transparency through explainability mandates and AI risk assessments.
3. Lead AI and data sovereignty discussions for emerging markets by establishing a Global South digital rights framework.
4. Accelerate cross-border data partnerships to drive economic growth while ensuring robust user protections.
5. Shape AI & Data Governance norms globally, ensuring ethical AI adoption in high-impact sectors like finance, healthcare, and governance.

India is at a pivotal inflection point. By strengthening regulatory accountability, AI fairness, and global digital partnerships, India can set a precedent for rights-driven, innovation-friendly, and globally influential data governance.

References

1. Baldwin, R. (2012). Regulation: Understanding regulation: Theory, strategy, and practice. Oxford University Press.
2. Bijker, W. E., & Law, J. (Eds.). (1992). Shaping technology/building society: Studies in sociotechnical change. MIT Press.
3. Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. Proceedings of Machine Learning Research 81:149-159, 2018 Conference on Fairness, Accountability, and Transparency. https://doi.org/10.48550/arXiv.1712.03586
4. California State Legislature. (2018). California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.100 et seq. Sacramento, CA: State of California. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
5. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998). https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
6. Commission Nationale de l'Informatique et des Libertés (CNIL). (2018). Solutions for a compliance approach with the GDPR for blockchain developers. CNIL. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data
7. Creemers, R. (2018). China's Social Credit System: An Evolving Practice of Control. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3175792
8. Dwork, C., Hardt, M., Pitassi, T., Reingold, O., & Zemel, R. (2012). Fairness through awareness. Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, 214-226. https://doi.org/10.1145/2090236.2090255
   European Data Protection Board. (2022). Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognize and avoid them. https://edpb.europa.eu/
9. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
10. European Union. (2023). Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. Official Journal of the European Union. https://eur-lex.europa.eu
11. European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending Regulations (EC) No 300/2008 and (EU) 2018/1139. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
12. Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970). https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act
13. Federal Trade Commission. (2022). Bringing dark patterns to light: An FTC report on deceptive digital design. https://www.ftc.gov
14. First Nations Information Governance Centre. (2014). Ownership, control, access, and possession (OCAP™): The path to First Nations information governance. First Nations Information Governance Centre. https://achh.ca/wp-content/uploads/2018/07/OCAP_FNIGC.pdf
15. Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160360. https://doi.org/10.1098/rsta.2016.0360
16. Forbes Advisor. (2024). MSME statistics and trends. Forbes. https://www.forbes.com/advisor/in/business/msme-statistics/
17. Fuller, L. L. (1964). The morality of law. Yale University Press.
18. General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://gdpr-info.eu/recitals/

19. General Data Protection Regulation, Regulation (EU) 2016/679, Article 23, 2016 O.J. (L 119) 1.
20. Government of India. (1950). The Constitution of India, Article 21: Right to life and personal liberty. Ministry of Law and Justice. https://legislative.gov.in/constitution-of-india
21. Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Electronics and Information Technology (MeitY). https://www.meity.gov.in/dpdp-act
22. Government of India. (2025). Draft Digital Personal Data Protection Rules, 2025. Ministry of Electronics and Information Technology (MeitY). https://www.meity.gov.in/dpdp-rules-2025
23. Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-6 (1996). https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
24. Indian Computer Emergency Response Team (CERT-In). (2022). Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedures, prevention, response, and reporting of cyber incidents for safe & trusted internet. Ministry of Electronics and Information Technology (MeitY), Government of India. Retrieved March 28, 2025, from https://www.cert-in.org.in
25. Infocomm Media Development Authority. (n.d.). Data Protection Trustmark (DPTM) certification. https://www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification
26. International Finance Corporation. (2024). Small business, big impact: Empowering women SMEs for success. https://www.ifc.org/en/stories/2024/small-business-big-impact
27. Latour, B. (2005). Reassembling the social: An introduction to actor-network-theory. Oxford University Press.
28. Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. Policy & Internet, 10(4), 415–453. https://doi.org/10.1002/poi3.183
29. Mashaw, J. L. (1997). Greed, chaos, and governance: Using public choice to improve public law. Yale University Press.
30. Ministry of Electronics and Information Technology (MeitY), Government of India. (2021). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The Gazette of India. https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf
31. Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
32. North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge University Press.
33. Organisation for Economic Co-operation and Development. (2020). The role of sandboxes in promoting flexibility and innovation in the digital age. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/06/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age_ddcd3d40/cdf5ed45-en.pdf
34. Ostrom, E. (1990). Governing the commons: The evolution of institutions for collective action. Cambridge University Press.
35. Press Information Bureau. (2025, February 4). Budget 2025-26: Fuelling MSME expansion. Government of India. Retrieved March 28, 2025, from https://pib.gov.in/PressReleasePage.aspx?PRID=2099687
36. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2018). Enhancing security and privacy in biometrics-based authentication systems. IBM Journal of Research and Development, 62(6), 1-12. doi: 10.1147/sj.403.0614
37. Rawls, J. (1971). A theory of justice. Harvard University Press.
38. Reserve Bank of India. (2022). Guidelines on digital lending: Implementation of recommendations of the working group on digital lending. https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3413
39. Securities and Exchange Board of India. (2023). Framework for AI-driven algorithmic trading in India. https://www.sebi.gov.in
40. Sen, A. (2009). The idea of justice. Harvard University Press.

41. Singapore Parliament. (2012). Personal Data Protection Act 2012 (No. 26 of 2012). Government of Singapore. https://sso.agc.gov.sg/Act/PDPA2012
42. Stein, M. A., & Lord, J. E. (2017). Accessibility, inclusion, and discrimination under international law. Cambridge University Press.
43. Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Writ Petition (Civil) No. 494 of 2012. https://digiscr.sci.gov.in/view_judgment?id=NjEwMg==
44. United Nations. (1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights
45. Tolbert, P. S., & Zucker, L. G. (1996). The institutionalization of institutional theory. In S. R. Clegg, C. Hardy, & W. R. Nord (Eds.), Handbook of organization studies (pp. 175-190). Sage Publications.
46. Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the Longwall method of coal-getting: An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social Structure and Technological Content of the Work System. Human Relations, 4(1), 3-38. https://doi.org/10.1177/001872675100400101
47. Tyler, T. R. (2006). Why people obey the law. Princeton University Press.
48. United Nations. (1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
49. U.S. Congress. (2022). Algorithmic Accountability Act of 2022, H.R. 6580, 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/6580
50. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Credits

OMI Foundation Trust is a new-age policy research and social innovation think tank operating at the intersection of mobility innovation, governance, and public good. Mobility is a cornerstone of inclusive growth providing the necessary medium and opportunity for every citizen to unlock their true potential. OMI Foundation endeavours to play a small but impactful role in ushering meaningful change as cities move towards sustainable, resilient, and equitable mobility systems which meet the needs of not just today or tomorrow, but the day after. OMI Foundation houses four interconnected centres that conduct cutting-edge evidence-based policy research on all things mobility:

1) **The Centre for Technology Transitions** is dedicated to transforming India's innovation ecosystem through a systems approach. It aims to position India as a global leader in ethical, inclusive, and sustainable technological innovation

2) **The Centre for Clean Mobility** catalyses the adoption of electric vehicles, future fuels, and renewable energy within the mobility ecosystem as a key climate strategy of cities.

3) **The Centre for Future Mobility** supports the leapfrog of cities to a sustainable future anchored in the paradigms of active, shared, connected, clean, AI-powered, and autonomous mobility.

4) **The Centre for Inclusive Mobility** promotes safe, accessible, reliable, and affordable mobility for all. It paves the road for the future of work and platform economy to fulfil the modern promise of labour.

Authors

Jagriti Arora, *Lead, Centre for Technology Transitions*

Jagriti approaches tech policy with curiosity and a readiness to question the status quo. With a degree in urban planning and additional training in technology policy through short-term courses, she brings a multidisciplinary perspective to complex challenges. Her experience spans policy research in mobility, the platform economy, Human-Computer Interaction (HCI), political consulting, and pedagogy, guided by research and first principles thinking.

Aishwarya Raman, *Executive Director, OMI Foundation*

An Oxford-trained sociologist, Aishwarya began her mobility sector journey as an entrepreneur and academic over a decade ago. A member of key policy committees at state, national, and global levels, she has received fellowships for AI-led transformations, including Salzburg Global and The Nippon Foundation fellowships. Under her leadership, OMI Foundation has developed pioneering policy tools, earning the organisation national and international recognition.

Suggested Citation

Arora, J. & Raman, A. (2025, April). *India's Digital Future: Strengthening DPDP Rules for Privacy, Innovation, and Global Leadership*. Position Paper. OMI Foundation.

Disclaimer

Neither OMI Foundation Trust nor its donor(s) nor any other party associated with this report will be liable for any loss or damage incurred by the use of this report.

Image Credits

Images for cover page, and table of contents created by the author on Gemini with ChatGPT-generated prompts.

For feedback and collaborations, email: comms@omifoundation.org

OMI FOUNDATION

https://omifoundation.org

https://x.com/OMIFoundation

https://linkedin.com/company/omi-foundation

https://www.instagram.com/omi.foundation

https://www.facebook.com/omifoundation.org

https://www.youtube.com/@OMIFoundation2023

Scan the QR code to view our website